STATE OF ALABAMA

Information Technology Standard

Standard 600-04S1: Incident Response Controls

1.   INTRODUCTION:

An incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. This State Standard provides the required controls for incident handling, reporting, and monitoring, as well as incident response training, testing, and assistance.

2.   OBJECTIVE:

Ensure State agencies are prepared to respond to cyber security incidents, to protect State systems and data, and prevent disruption of government services.

3.   SCOPE:

This Information Technology Standard applies to all users (State of Alabama employees, contractors, vendors, and business partners) of any State-managed information system resources.

4.   REQUIREMENTS:

Based on the recommendations of the National Institute of Standards and Technology (NIST) found in Special Publication 800-53: Recommended Security Controls for Federal Information Systems, State of Alabama cyber security incident response programs shall implement the following controls:

4.1   INCIDENT RESPONSE CONTROLS FOR ALL SYSTEMS

The following controls are applicable to all State of Alabama information systems:

4.1.1   Incident Response Policy and Procedures

Organizations that support information systems shall develop, disseminate, and periodically review/update:

(i) a formal, documented, incident response policy that addresses purpose/objective, scope, roles and responsibilities, and compliance/enforcement (State IT Policy 600-04 and this Standard satisfy this requirement); and

(ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

Incident response procedures shall be developed for the security program in general and as required for particular information systems.

4.1.2 Incident Handling

Organizations that support information systems shall implement an incident handling capability for cyber security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

Incorporate the lessons learned from prior and ongoing incident handling activities into the applicable incident response procedures.

4.1.3 Incident Reporting

Promptly report cyber security incident information to appropriate authorities in accordance with State or organization incident reporting procedures.

Ensure the types of incident information reported, the content and timeliness of the reports, and the list of designated reporting authorities or organizations are consistent with applicable laws, directives, policies, regulations, standards, and procedures.

4.1.4 Incident Response Assistance

Organizations that support information systems shall provide an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. This support resource shall be an integral part of the organization's incident response capability.

Possible implementations of incident response support resources in an organization include a help desk or an assistance group and, when required, access to forensics services.

4.2 ADDITIONAL CONTROLS FOR HIGH IMPACT SYSTEMS OR DATA

Organizations supporting incident response capabilities for high impact (see Definitions) systems or data shall further enhance all of the above control requirements by employing automated mechanisms where possible. The following additional controls shall also be applied:

4.2.1 Incident Response Training

Organizations shall train personnel in their incident response roles and responsibilities with respect to the information systems they support. Provide annual refresher training.

4.2.2 Incident Response Testing

Organizations shall test the incident response capability for the information systems they support at least annually using organization-defined tests, simulated events, and exercises to determine the incident response effectiveness. Document the results.

4.2.3 Incident Monitoring

Organizations shall track and document information system security incidents on an ongoing basis.

Possible implementations of ongoing monitoring include automated monitoring and alerting systems, automatic notifications, and incident metrics.

5.   DEFINITIONS:

HIGH IMPACT: The potential impact is HIGH if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Adverse effects on individuals may include, but are not limited to, loss of the privacy to which individuals are entitled under law.

A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

(i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;

(ii) result in major damage to organizational assets;

(iii) result in major financial loss; or

(iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

[Source: FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems]

6.   ADDITIONAL INFORMATION:

6.1   POLICY

Information Technology Policy 600-04: Cyber Security Incident Response

6.2   RELATED DOCUMENTS

Information Technology Procedure 600-04P1: Incident Reporting

Information Technology Procedure 600-04P2: Incident Handling

Signed by Eugene J. Akers, Ph.D., Assistant Director

Revision History

Version	Release Date	Comments
Original	1/12/2007	